WORKSTATION USE AND SECURITY PROCEDURES

The Department of Mental Health Chief Information Officer (DMH CIO) or his/her designee must ensure that the following workstation security procedures are implemented within each Department of Mental Health (DMH) facility. "Workstations" include County and personal computers, mobile devices - e.g., tablet personal computers (PCs), personal digital assistants (PDAs), cellular telephones, computer carts-modems, printers, and fax machines, etc., that are used for County business.

1. Workstation Use

These procedures include documented instructions delineating the proper functions to be performed by DMH Workforce Members and the manner in which those functions are to be performed (e.g., logging off before leaving a workstation unattended) to maximize the security of health information.

A. Access and Use of Workstation and Network Services

Measures to limit unauthorized access must include the following:

1. Configuration of workstations and network services.

   a. System Managers/Owners must configure workstations and network services to allow only authorized access to the workstation and network services (e.g., data, applications, intranet, and Internet).

   b. Workforce Members must have both authorization to access a workstation and the appropriate rights to do so. Users must not access any confidential and/or sensitive information from a workstation unless they have authorization to do so and it is necessary for doing their job.

2. Permitting only authorized access to workstations and network services through the use of controls.

   The DMH CIO or his/her designee, taking into consideration each system's Risk Analysis Sensitivity Score, is responsible for the creation, design, and implementation of measures to limit unauthorized access by Workforce Members to workstations and network services.

   a. Unique User IDs and Passwords

      i. The DMH CIO or his/her designee is responsible for ensuring the assignment of a unique User 10 to each user, to identify and track the user's identity when logging into workstations, networks, or applications.

      ii. Each user must protect his/her password. Users must not write down their password and place it at or near the workstation (e.g., a note taped to the monitor or placed under the keyboard).

      iii. Logging into workstations, networks, or applications with another user's 10 and/or password is prohibited.

iv. Users must not share their unique User IDs (logon/system identifier) with any other person.

v. Users' passwords must be changed at least once every ninety (90) days.

vi. Passwords must be at least eight (8) characters long and contain a combination of alpha and numeric characters. The password may also include special characters.

vii. Two-factor authentication in which the user provides two means of identification, one typically a physical token (e.g., a card) and the other typically something memorized, (e.g., a security code) must be used for information systems receiving a Risk Analysis Sensitivity score of "High."

(Refer to DMH Policy No. 550.01, Security Management Process: Analysis Procedure to determine the Risk Analysis Sensitivity Score.)

b. Other User Authentication Methods

With authorization from the DMH Departmental Information Security Officer (DISO) may utilize other user authentication methods (e.g., badge readers, biometric devices, tokens).

3. Access to Workstations Not in Use

a. Workstations not in use must be password protected and locked.

b. Workstations must be set up to generate a password-protected screen saver when the computer receives no input for a specified period of time (to be determined by the DMH CIO based on the result of the risk assessment). The DMH CIO or his/her designee may approve other "lockout" schemes that protect against the unauthorized access to confidential and/or sensitive information.

4. Workstations must display an appropriate warning banner prior to gaining operating system access.

2. Access and Use of Mobile Devices

A. Mobile devices must be pre-approved and registered for use in a facility by the DMH CIO or his/her designee.

B. Workforce Members must exercise good judgment in determining the amount of necessary data stored on their mobile devices to perform their functions.

C. Access to mobile devices must be protected at all times consistent with the procedures set forth in **1. Workstation Use,** A. Access and Use of Workstation and Network Services section above.

D. Mobile devices containing sensitive information (e.g., confidential patient information) must be encrypted.

E. When traveling, a Workforce Member must not leave mobile devices unattended in non-secure areas.

F. Mobile devices that are left in cars must be stored out of sight, and the car must be locked.

3. Physical Attributes of Surroundings

Workforce Members must be aware of the physical attributes of the surroundings where the workstation is located. Precautions need to be taken to prevent unauthorized access of unattended workstations, to automatically erase sensitive information left displayed on unattended workstations, and to limit the ability of an unauthorized individual to observe sensitive information when a workstation is in use by a user. The following measures must be taken:

A. Confidential data (e.g., patient information) must be password protected, encrypted, or stored on a secure network drive.

B. Confidential data having a Sensitivity Score of "High" must be encrypted.

C. Confidential data must not be downloaded without authorization from the DMH CIO or his/her designee.

D. Confidential data must not be saved on removable devices (e.g., floppy disk, Compact Disc Read Only Memory (CD-ROM), external drives, Universal Serial Bus (USB) drives) without proper safeguards and authorization from the DMH CIO or his/her designee. Removable media containing confidential data (e.g., patient information) must be maintained and stored in secured areas.

E. Printers are not to be left unattended in non-secure areas when printing confidential and/or sensitive information.

F. Disposal of confidential electronic records stored on removable or external media (e.g., CDROM, diskettes, hard drives) must be in accordance with DMH Policy No. 554.01, DMH Device and Media Controls Policy.

G. Use caution when viewing and entering confidential information.

H. Layout and design of the space must shield the view of the workstation screen from the public, unless the requirements of subsection B. Hardware/Software, 4., below, apply and are complied with.

I. Where it is not possible, through layout and design of the space, to shield the workstation screen from view, devices like privacy screens and shields are to be used.

4. Workstation Security

These procedures are intended to put in place physical safeguards to restrict access to information through securing DMH workstations.

A. General

1. Workstations located in public or open areas must be physically secured in a locked room, secured in locked cabinets, or strongly anchored to deter unauthorized movement. Security cameras or additional forms of monitoring should be considered in high-risk areas.

2. Mobile devices must be secured when not in use. These devices must either be carried on persons or must be stored in secured areas.

3. Workstation equipment must not be removed from the premises unless documented and pre-approved by the user's supervisor.

4. Devices must be located in environments that are in accordance with the equipment manufacturer's operational specifications.

5. Inventory and maintenance records must be maintained for all workstations.

6. Computer monitors must be positioned away from common areas, or a privacy screen must be installed to prevent unauthorized access or observation in accordance with DMH Policy No. 508.01, Safeguards for Protected Health Information (PHI).

B. Hardware/Software

1. Workforce Members must not change the system configuration of their workstation (e.g., network properties, video card) without proper authorization.

2. Workforce Members must not install or uninstall software (e.g., downloaded Internet software, games, patches, plug-ins, screen savers) on their workstation without proper authorization and licensing.

3. Only authorized users may install/uninstall software and perform repair services on workstations.

4. Workforce Members must not re-enable floppy drives, CD-ROM drives, USB ports, etc., on workstations that have access to confidential data, unless the Workforce Member is authorized to use those drives.

5. The Facility Manager/Program Head or his/her designee must ensure that appropriate controls are in place when sending equipment off premises for maintenance (i.e., the maintenance contract must include business associate language).

6. All hardware and software connected to a facility's network services must be managed centrally within each facility.